Department of Homeland Security Daily Open Source Infrastructure Report for 27 December 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Times reports that drug manufacturer Roche said larger doses of the anti−viral drug Tamiflu may be needed to treat avian flu after evidence emerged of resistance to the drug. (See item 20)
- Wayne County, Michigan, has launched a system to provide alert notifications to 42 cities, towns and jurisdictions over a common communications platform, and plans to include alerts from more than 300 chemical plants in the future. (See item 23)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *December 23, Reuters* — **Fire out at Nigeria pipeline.** Firefighters have put out a blaze caused by a suspected dynamite attack at two pipelines operated by Royal Dutch Shell in remote southern Nigeria and workers are fixing them, a Shell spokesperson said on Friday, December 23. Output is still down by 180,000 barrels per day (bpd) and a force majeure is still in place, the spokesperson said, three days after unknown gunmen attacked the pipelines in the Opobo channel in the Niger Delta, killing 11 people. "The fire is out. We've finished repairs on the 24−inch pipeline and we'll commence repairs on the 28−inch one today," a company spokesperson in Lagos said. He added that two oilfields that were closed to help curb the fire were still down. The two pipelines carry crude oil from different fields to the Bonny Light

export terminal. Shell's act of force majeure, a technical release from honoring contracts, is expected to delay delivery of more than 300,000 bpd of crude for nearly a week.
Source: http://abcnews.go.com/US/wireStory?id=1436194

2. *December 23, KOTV (OK)* — **Plane clips power lines.** The lights are back on in east Tulsa, OK, after a small plane clipped some power lines near a small airport. The incident occurred on Thursday, December 22, and power went out to 2,000 customers for a little over an hour. Witnesses heard the plane snap the wires before the plane landed safely at Harvey Young Airport.
Source: http://www.kotv.com/main/home/stories.asp?whichpage=1&id=959 11

3. *December 22, Associated Press* — **El Paso pipelines below pre−storm levels.** Natural gas distributor El Paso Corp. on Thursday, December 22, said its pipeline systems are still operating below their levels before hurricanes Katrina and Rita struck in late August and September. Total natural gas flow is down by 770 million cubic feet. El Paso said its ANR pipeline is pushing through about 200 million cubic feet less natural gas than normal, while its Southern natural gas line is operating at 170 million cubic feet less and its Tennessee natural gas line is running at about 400 million cubic feet less. The availability of third−party production and processing facilities is still hindering flow at the Tennessee pipeline, El Paso said.
Source: http://biz.yahoo.com/ap/051222/el_paso_hurricane_update.html ?.v=1

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *December 23, Engineering News−Record* — **President signs terrorism insurance extension.** President Bush has signed into law a bill to continue the federal terrorism insurance program for two years. The program had been set to expire December 31. The bill extends the 2002 Terrorism Risk Insurance Act through December 2007, assuring that federal "backstop" coverage for major terrorism−related claims will continue, but the new measure requires insurers to pick up a larger share of the risk. The legislation increases the size of a terrorist event that activates the federal coverage from the current level of $5 million in insured claims to $50 million in 2006 and then to $100 million in 2007. The measure also hikes the amount of claims that insurers would have to cover, from 15% of premiums now, to 17.5% in 2006 and 20% of premiums in 2007. Moreover, the legislation eliminates some insurance lines from

potential backstop coverage, including commercial automobiles, professional liability, burglary and theft, surety, multiple peril and farm owners.
Source: http://enr.ecnext.com/coms2/summary_0271−23783_ITM

5. *December 22, Commonwealth of Pennsylvania* — **Pennsylvania governor signs identity theft bill.** Pennsylvania Governor Edward G. Rendell on Thursday, December 22, signed Pennsylvania Senate Bill 712 into law to better protect Pennsylvanians after their personal information is lost or stolen from computer systems. SB 712 establishes the "Breach of Personal Information Notification Act" and says a state agency, political subdivision, individual or business that operates in Pennsylvania and maintains, stores or manages personal consumer information on computer, must notify people if their security systems are breached. Personal information under the bill includes an individual's first name, or initial, and last name; social security number; driver's license, or state−issued identification number; or a financial account number. The bill becomes effective 180 days after signing.
Source: http://www.governor.state.pa.us/governor/cwp/view.asp?a=1115 &q=444594

6. *December 22, The Scotsman (Scotland)* — **Credit cards fraud gang set up fake store in Scotland.** A gang set up a fake shop selling Scottish trinkets as cover for a major scheme to make thousands from credit card fraud. The gang, which had links to Edinburgh, raked in nearly US$34,000 in a week by skimming the credit cards of unsuspecting bank customers across the UK. They then used the cards' details at a gift shop they had set up in Perth for the sole purpose of completing the fraud. The court heard how the gang set up a device on ATM machines to read people's card details. The gang member who fronted the shop set up the fake "Gift Shop UK" in Perth to process fraudulent sales using the copied cards.
Source: http://news.scotsman.com/scotland.cfm?id=2448972005

7. *December 21, Financial Crimes Enforcement Network* — **Final regulation implementing Section 312 of the USA PATRIOT Act announced.** The Financial Crimes Enforcement Network (FinCEN) announced on Wednesday, December 21, a final regulation implementing the international correspondent banking provisions and the private banking provisions of Section 312 of the USA PATRIOT Act. The final rule requires certain U.S. financial institutions to apply due diligence to correspondent accounts maintained for certain foreign financial institutions. "This rule reflects a significant milestone in our continued progress towards adding transparency to the financial system to help safeguard it from the financing of terror and other illicit money flows," said William J. Fox, FinCEN Director. The final rule implements all of Section 312 with the exception of the provisions requiring enhanced due diligence in connection with certain foreign correspondent banks. With respect to correspondent banking generally, it limits the scope of U.S. financial institutions to which the rule applies and outlines the general due diligence requirements. With respect to private banking accounts, the final rule similarly limits the scope of U.S. financial institutions to which the rule applies, outlines the due diligence and enhanced due diligence that is required, and further clarifies duties with respect to accounts maintained for senior foreign political figures.
Final Rule: http://www.fincen.gov/312finalrule.pdf
Source: http://www.fincen.gov/section312.pdf

[Return to top]

Transportation and Border Security Sector

8. *December 23, New York Times* — **With deal reached, normal commutes return to New York.** While buses on some routes seemed to be operating less frequently than normal Friday, December 23, the nation's largest transit system −− which carries more than seven million riders each day −− was back up, much to the relief of riders. The return of public transit meant the end of shared cab rides, in which taxis charged a flat fee of $10 or $20 per passenger; the end of 3:30 a.m. EST traffic jams as commuters rushed into Manhattan before 5 a.m. carpool rules took effect; and the resumption of alternative side parking rules. The abrupt return of workers on Thursday, December 22 −− many strikers simply laid down their placards and walked into the buildings they had been picketing −− capped a day of fast−moving developments in a labor showdown that just a day before seemed headed for an intractable and ugly stalemate. Despite the end of the strike, a final settlement of the dispute remains to be reached. The strike −− the city's first transit walkout in a quarter−century −− paralyzed New York's mass transit system at the height of the holiday season, devastating sales for retailers, enraging the mayor and governor and making it hellishly difficult for New Yorkers to get to jobs, schools and doctors' appointments.
   Source: http://www.nytimes.com/2005/12/23/nyregion/nyregionspecial3/ 23cnd−strike.html

9. *December 23, New York Times* — **Seaplane fleet to be tested for metal fatigue after crash.** Now that it appears obvious that the Grumman Mallard seaplane that crashed Monday, December 19, off Miami had metal fatigue, the airline and the Federal Aviation Administration are devising a way to inspect the four remaining Mallards for the same problem. But the difficulty they face may illustrate why the problem was not discovered in the plane before it crashed. Mark V. Rosenker, acting chairman of the National Transportation Safety Board, said Thursday, December 22, that getting to the wing beam that came apart in the crash would require peeling back the metal skin of the plane. Fatigue can be found by a variety of inspection techniques, experts say, and the spot where it was found in the wreckage, on the spar, an internal beam near the fuselage, is the first place to look, said George H. Kizner, chairman of the mechanical engineering department at Vaughn College of Aeronautics and Technology, in Queens. The safety board is probably months away from concluding that metal fatigue was the immediate cause of the Miami crash.
   Source: http://www.nytimes.com/2005/12/23/politics/23plane.html?page wanted=all

10. *December 23, Associated Press* — **Delta will shut down two−thirds of gates at Orlando.** Delta Air Lines said Friday, December 23, it plans to shut down two−thirds of its gates at Florida’s Orlando International Airport as part of attempts to emerge from bankruptcy. Delta will close 16 of its 24 gates at the airport on January 18, said Anthony Black, a company spokesperson. "It's part of our overall efforts to restructure our costs and to get them in line with our operations," Black said. "The bankruptcy process has afforded us the opportunity to address the situation of having too many gates." Delta and its subsidiaries, including Song and Comair, currently operate 115 flights from the airport each day, Black said. Despite the airline's lease cancellation, Black said the company plans to increase the number of flights moving through the Orlando airport.
    Source: http://www.usatoday.com/travel/news/2005−12−23−delta−orlando_ x.htm

[Return to top]

Postal and Shipping Sector

11. *December 24, Associated Press* — **Inmate accused of making anthrax threat to Kentucky post office.** A Texas man serving a 60−year prison term has been indicted on charges that he threatened to poison a Kentucky post office with anthrax. James Richard Cunningham is accused of writing a threatening communication to the postmaster in Bowling Green. Cunningham was indicted by a U−S District Court grand jury on Wednesday, December 21. He is in prison after pleading guilty last December to robbery, burglary, and two counts of aggravated sexual assault.
Source: http://www.lex18.com/Global/story.asp?S=4285248&nav=EQlp

[Return to top]

Agriculture Sector

12. *December 23, News and Sentinel (WV)* — **West Virginia chronic wasting disease outbreak small in scale.** West Virginia's chronic wasting disease (CWD) outbreak appears to be confined to a small section of Hampshire County, state Division of Natural Resources officals said. Nearly 1,000 hunter−killed deer sampled in Hampshire County during hunting season tested negative for the brain−destroying disorder. The first infected deer was discovered in September and a few more infected deer were found in a group of more than 200 deer Division of Natural Resources (DNR) officials killed in the area where the first infected deer was found. During the November deer season, the agency sampled deer killed by hunters in a countywide sample. None of those tested positive. Paul Johansen, the DNR's assistant wildlife chief, said the disease outbreak appears to be limited to a small area around Slanesville in Hampshire County. Johansen said the DNR's next step would be to map the area where all the CWD−positive animals were found.
CWD information: http://www.cwd−info.org/
Source: http://www.newsandsentinel.com/news/story/1223202005_new10_c hronic122305.asp

13. *December 22, Niles Star (MI)* — **Farm plan updated.** Farm managers need to be prepared to respond if an emergency occurs, whether it's due to bioterrorism, a natural disaster, or an accident. Michigan State University Extension and the Michigan Groundwater Stewardship Program recently updated a bulletin called “Emergency Planning for the Farm” (bulletin E−2575) that can help producers plan for incidents and accidents. A farm emergency plan contains emergency contact information, farmstead and aerial maps, and information for handling fertilizer, pesticide and manure spills, fires, and other emergency or suspicious activities. Firefighters, rescue teams, and other responders use the plan to determine quickly if any farmstead hazard exists that may deter rescues or endanger human lives. Every farmer is encouraged to maintain an up−to−date inventory of stored products −− pesticides, fertilizers, and farm flammables −− and their storage locations, along with a list of the farm's and the nearby emergency equipment and supplies. Updated emergency plans should be dated and filed in at least four locations: in the farm office, in the emergency tube, in farm vehicles/tractors, and with the fire department or local emergency planning committee .
Source: http://www.nilesstar.com/articles/2005/12/22/news/ndnews3.tx t

[Return to top]

Food Sector

14. *December 23, U.S. Food and Drug Administration* — **Fruit recalled.** The U.S. Food and Drug Administration (FDA) has announced the recall of some shipments of ackee −− a tropical fruit imported from Jamaica −− because the fruit has levels of a naturally occurring toxin called hypoglycin that are of health concern. The recall involves 31 cases of Ashman's Ackees in Brine, distributed by Harvest Foods, Hartford, CT. The products were shipped in early November to one wholesaler in New York, and to retail stores and restaurants in New York, Massachusetts, and Connecticut. No illnesses have been reported to FDA concerning the Harvest Foods product. The ingestion of under−ripe ackee has been linked to sudden vomiting. Infrequently, high levels of hypoglycin can lead to convulsions, coma, and death. Hypoglycins in the ackee are found in toxic levels when the fruit is picked too early and is under−ripe.
Source: http://www.fda.gov/bbs/topics/news/2005/NEW01288.html

15. *December 22, Animal and Plant Health Inspection Service* — **Importation of Chinese fragrant pears allowed.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service is amending its fruits and vegetable regulations to allow, under certain conditions, the importation of fragrant pears from China. To be eligible for importation, the pears must be grown in the Korla region of Xinjiang Province at a production site that is registered with the national plant protection organization of China. The fragrant pears are subject to both pre−harvest and post−harvest inspections. In addition, the pears must be packed in insect−proof containers that are labeled in accordance with the regulations and safeguarded from pest infestation during transport to the U.S.
Source: http://www.aphis.usda.gov/newsroom/content/2005/12/chipears_ppq.shtml?PC_7_2_5JM_contentid=2005/12/0551.xml&PC_7_2_5JM_navtype=RT&PC_7_2_5JM_parentnav=LATEST_RELEASES&PC_7_2_5JM_navid=NEWS_RELEASE#7_2_5JM

16. *December 22, Associated Press* — **Japan mid−sized grocers to sell U.S. beef.** Japan's mid−sized supermarkets will be the first to restock U.S. beef −− at substantial markups −− following the lifting of the country's two−year import ban, a news report said Friday, December 23, as major chains take a wait−and−see approach. Mid−sized grocers in the northern prefecture of Hokkaido and on the western island of Shikoku are among those planning to start selling North American beef again, at a total of more than 100 stores, the Nihon Keizai newspaper said. Prices are expected to be 20 percent to 30 percent higher than they were before the meat was banned in 2003, the report said. Japan partially lifted the two−year ban on U.S. beef imports on December 12. Japan had been the most lucrative export market for American ranchers before they were shut out following the first case of mad cow disease in the U.S. herd. Some restaurants are still reluctant to market American meat, while major supermarket chains are also cautious.
Source: http://www.businessweek.com/ap/financialnews/D8ELLDQG0.htm?campaign_id=apn_asia_up&chan=gb

17.

December 22, Associated Press — **Chili dogs recalled.** Scobee Foods Inc. of Dallas, TX, has recalled 364 packages of Double Chili Dogs with Cheese because they could potentially be contaminated with Listeria monocytogenes, an organism that can cause fatal infections in young children or people with weakened immune systems. The product was distributed in Dallas and Grand Rapids, MI, through vending machines and convenience food stores. No illnesses have been reported, the company said in a release Thursday, December 22. The recall is the result of a routine sampling program by Texas health officials that revealed that the finished products contained the bacteria.
Source: http://www.dfw.com/mld/startelegram/news/state/13468197.htm

18. *December 22, Associated Press* — **Warning issued about potential rabies in raw milk.** The Oklahoma state Health Department says anyone who drank raw, unpasteurized milk or cream sold by Swan Brothers Dairy in Claremore earlier this month may have been exposed to rabies. One cow at the farm has been confirmed to have rabies and its milk was combined with milk from healthy cows and sold from December 4 through the 19. Health officials say most healthy persons who drank the milk or cream are not at risk, but people with certain medical conditions should contact their doctor to determine if rabies shots are needed. Those conditions include suppressed immune systems and abnormalities of the palate, mouth, throat, or esophagus. Rabies is usually transmitted through a bite or saliva into an opening in the skin. There are no documented cases of human rabies due to drinking milk from a rabid animal, but a small risk is thought to exist.
Source: http://www.kotv.com/main/home/stories.asp?whichpage=1&id=958 85

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

19. *December 25, Associated Press* — **New England redistributes flu vaccines.** Health officials across New England are shuffling flu vaccine shots from hospitals and clinics with oversupplies to those facing shortages. In Massachusetts, 7,000 to 10,000 doses of flu vaccine have been shipped back to the state Department of Public Health for redistribution to facilities facing short supplies. Connecticut's state health agency is helping clinics with too much vaccine send their supplies to centers facing shortages. For example, a visiting nurse agency in Connecticut sent 950 flu shot doses to the Navajo Area Indian Health Service for distribution in New Mexico. The shots were shipped via overnight delivery service after Navajo health officials issued a nationwide plea for surplus vaccine. Millions of flu shots tailored to predicted flu strains are distributed annually in the U.S. from October through January by both government agencies and private companies. It's a patchwork system that some public health officials say is in need of reform. The U.S. Centers for Disease Control and Prevention this month inaugurated a system that allows state health authorities to access a secure computer network with information about vaccine deliveries to a particular ZIP code. Public health officials say the

system only gives them a rough idea of how much vaccine is in their states.
Source: http://abcnews.go.com/Health/wireStory?id=1441438

20. *December 23, Times (United Kingdom)* — **Flu drug dose may need boosting after signs of resistance.** Larger doses of the anti−viral drug Tamiflu may be needed to treat avian flu, the drug manufacturer Roche said Thursday, December 22, after evidence emerged of resistance to the drug. It may also be necessary to combine the drug with other antiviral agents to treat the H5N1 avian virus, the company said. A study published in the New England Journal of Medicine, highlighted the deaths of two Vietnamese girls who had become resistant to Tamiflu despite getting the current full dose of treatment. The immediate relevance of the finding to a potential world pandemic of flu was not clear. Any pandemic strain will be easier to catch but less virulent than H5N1, and trials of Tamiflu against seasonal flu have shown that in a small proportion of cases, resistance does develop. For adults, the rate of resistance is about 0.4 percent, and for children under 12, about four percent. The resistant virus is less virulent than the unaltered type, so if Tamiflu is ineffective in these cases it may not matter much.
Study: http://content.nejm.org/cgi/content/full/353/25/2667
Source: http://www.timesonline.co.uk/article/0,,25149−1957703,00.htm l

21. *December 23, Associated Press* — **World Health Organization calls on China to release flu samples.** A senior World Health Organization (WHO) official appealed to China to hand over samples of the H5N1 bird flu virus, saying Friday, December 23, that Beijing has failed to release any samples from its dozens of outbreaks in poultry this year. WHO's Asia−Pacific Director Shigeru Omi said that sharing virus samples is crucial to diagnosing new cases, and to developing a vaccine that could prevent a possible pandemic in humans. "From the more than 31 reported outbreaks in animals from 2005, no (Chinese) viruses have been made available so far for the international community," Omi said. "Time is of the essence." China's Ministry of Health agreed this week to give the WHO samples isolated from two of its six confirmed human cases of bird flu. Scientists have determined that bird flu strains in Vietnam and Thailand resemble each other, while a distinct second strain has affected birds in China and Indonesia. A potential third strain may have affected birds and sickened at least one human in northeast China's Liaoning province, Omi said.
Source: http://www.cbsnews.com/stories/2005/12/23/ap/world/mainD8ELV L0O0.shtml

22. *December 22, Agence France−Presse* — **China begins human trials of bird flu vaccine.** China began human trials of a bird flu vaccine this week, giving six Chinese volunteers shots of the experimental immunization against the deadly virus, state media said. The volunteers, who were given shots of the vaccine Wednesday, December 21, are the first batch of 120 volunteers chosen from healthy people between the age of 18 to 60 from Beijing. The vaccine is jointly developed by the Beijing−based pharmaceutical company Sinovac Biotech Co. and the Chinese Center for Disease Control and Prevention. The experiments will last nine months, but preliminary conclusions are expected in around three months.
Source: http://news.yahoo.com/s/afp/20051222/hl_afp/healthfluchinava ccine_051222191220;_ylt=Apy0W.fqHj2kYgLhRGvvGfaJOrgF;_ylu=X3 oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

23. *December 23, Computer World* — **Michigan county expands emergency communications interoperability.** Communications interoperability is a problem facing nearly all of the nation's 50,000 emergency response authorities that will take years to fix. But Wayne County, MI, has already launched a system to connect 42 different cities, towns and jurisdictions over a common communications platform and is moving to the next step to include more than 300 chemical plants. The county, with a population of 2.2 million that includes Detroit, began its journey to link different radios, cell phones, laptops and data handhelds more than two years ago. The system provides both interoperability and alert notification to business and residents, and will soon be expanded to take alerts from the many chemical plants in the area, he said. One especially useful part of the system is that Wayne County can alert various jurisdictions quickly and securely when the Department of Homeland Security raises its security threat rating, so that jurisdictions know to lock doors and add guards to power plants and water supplies, Hammond said. Before, the various jurisdictions were not always sure the change in the threat rating was legitimate.
Source: http://www.computerworld.com/mobiletopics/mobile/story/0,108 01,107348,00.html

24. *December 23, Indian Express* — **India putting in place indigenous tsunami warning system.** A year after the tsunami of December 26, 2004, India is moving to put in place its own tsunami−warning system, for which the government insists it will not use overseas help and which will be ready by September 2007. Under the ambitious plan, India will install tsunami warning sensors close to the ocean floor at appropriate locations in the Indian Ocean with real−time connectivity and will create a network of tide gauges and data buoys to determine the time when tsunami waves could hit land. The 24/7 tsunami early warning center will be housed at the Indian National Center for Ocean Information Services (INCOIS), in Hyderabad, and will be a multi−hazard monitoring point that will also look at the storm surges that develop due to cyclones. To bolster already−existing monitoring networks, the Indian government wants to augment the 12 online tide gauges with 50 more, eight of which are now online. It also plans to hike the number of seismic stations from 51 to over 170. India’s objective is to bring down the time taken for assessing earthquake parameters from the current 40 minutes to 10 minutes.
Source: http://www.indianexpress.com/full_story.php?content_id=84510

25. *December 22, U.S. Department of State* — **U.S. provides hazard warning expertise to Indian Ocean nations.** The yearlong international effort to secure Indian Ocean coastal populations against the ravages of another deadly tsunami is paying off, as members of the International Oceanographic Commission (IOC) Intergovernmental Coordination Group (ICG) converge on basic principles of an operational early warning system for the region. Through the U.S. Indian Ocean Tsunami Warning System (IOTWS) program, U.S. agencies will spend $16.6 million over two years to help develop early warning capabilities for tsunamis and other hazards in the Indian Ocean. The U.S. National Oceanic and Atmospheric Administration (NOAA) has been a

major technical adviser to the IOC−ICG. One of NOAA's main goals, said Curt Barrett, director of the Indian Ocean Project, is to work with the World Meteorological Organization (WMO) to improve the region's segment of a meteorological communication system called the Global Telecommunications System (GTS). U.S. agencies also participated as observers and technical advisers during a December meeting in Hyderabad, India, the second session of the IOC−ICG for the IOTWS. Out of the consensus, emerged an outline for implementing the Indian Ocean system. The IOC plans use the outline to write a draft of the implementation document within 60−90 days.
For additional information on the IOTWS:
http://usinfo.state.gov/gi/Archive/2005/Dec/22−831749.html
Source: http://usinfo.state.gov/usinfo/Archive/2005/Dec/22−941039.ht ml

26. *December 22, Associated Press* — **Group to work together for earthquake preparedness.** Arkansas Congressman Marion Berry (D−AR) and others have formed a working group to prepare the New Madrid fault region for a possible earthquake. Berry says the country cannot afford to let another natural disaster catch everyone off guard. The New Madrid faults extend from southern Illinois into northeastern Arkansas. In 1811 and 1812, powerful earthquakes shook the South, forming Tennessee's Reelfoot lake and causing the Mississippi River to run backward. The New Madrid Earthquake Congressional Working Group will help develop emergency plans and improve regional communication in case of an earthquake. Members include Jo Ann Emerson (R−MO), Roger Wicker (R−MS), Harold Ford Junior (D−TN), and John Tanner (D−TN). Berry's office says the group doesn't yet have dedicated funds, and that will be one of the first steps.
Source: http://www.todaysthv.com/news/news.aspx?storyid=22127

[Return to top]

Information Technology and Telecommunications Sector

27. *December 23, NewsFactor Magazine Online* — **Gartner warns about Microsoft Vista metadata problem.** Windows Vista, the next version of Microsoft's Windows client operating system, will give users the ability to search for files by looking for information in the file's metadata tags. However, a report by IT research firm Gartner warned that allowing users to search for metadata tags in this manner could result in private information being inadvertently disclosed. Metadata consists of "data about data." It is supplementary information about the author of a document, its various revisions, and any changes that have been made, explained Neil MacDonald, Gartner's vice president and distinguished analyst of information security, privacy, and risk. The Gartner report, "Plan To Deal with Metadata Issues with Windows Vista," written by MacDonald and Gartner analyst Michael Silver, outlines one example in which an employee might give a document about a client the metadata tag "bad client." If that document were then sent to the client, considerable embarrassment, even loss of business, could result. The Gartner report suggested that firms must have a strategy in place for dealing with metadata before adopting Windows Vista.
The referenced Gartner report is available for purchase: http://www.gartner.com/
Source: http://www.newsfactor.com/news/Gartner−Warns−About−Vista−Met adata/story.xhtml?story_id=113003ORER88

28. *December 22, Security Focus* — **Apple Mac OS X KHTMLParser remote denial of service vulnerability.** Apple Mac OS X KHTMLParser is affected by a remote denial of service vulnerability. Successful exploitation may cause an application employing KHTMLParser to crash. KHTMLParser is used by Apple Safari Web browser and Apple TextEdit word processor.
Source: http://www.securityfocus.com/bid/16045/references

29. *December 22, Security Focus* — **Linux kernel ICMP_Push_Reply remote denial of service vulnerability.** Linux kernel is prone to a remote denial of service vulnerability. Remote attackers can exploit this to leak kernel memory. Successful exploitation will result in a crash of the kernel, effectively denying service to legitimate users. Solution: Linux kernel version 2.6.12.6 has been released to address this issue. Ubuntu Linux has released advisory USN−231−1, along with fixes to address various kernel issues. For further solution detail refer to: http://www.securityfocus.com/bid/16044/solution
Source: http://www.securityfocus.com/bid/16044/references

30. *December 22, Security Focus* — **McAfee VirusScan path specification local privilege escalation vulnerability.** McAfee VirusScan is prone to a vulnerability that could allow an arbitrary file to be executed. The 'naPrdMgr.exe' process calls applications without using properly quoted paths. Successful exploitation may allow local attackers to gain elevated privileges. Solution: It has been reported that McAfee VirusScan Enterprise 8.0i patch 12 is not vulnerable to this issue. This could not be confirmed by Symantec.
Source: http://www.securityfocus.com/bid/16040/references

31. *December 22, Security Focus* — **Linux kernel local socket buffer memory exhaustion denial of service vulnerability.** Linux kernel is susceptible to a local denial of service vulnerability. The issue is due to a failure of the kernel to properly check and enforce memory resource constraints. This is triggered by consuming excessive kernel memory by creating multiple sockets with large kernel buffers; this allows local attackers to consume excessive kernel memory, eventually leading to an out of memory condition, and a denial of service for legitimate users.
Source: http://www.securityfocus.com/bid/16041/references

32. *December 22, CNET News* — **British "rogue dialers" face heftier fines.** British Parliament members have agreed to raise the maximum fine that can be imposed against companies that operate "rogue dialer" software that hijacks a dial−up Internet user's Web connection. Parliament on Wednesday, December 21, agreed that, as of Friday, December 30, companies caught abusing United Kingdom premium−rate services should be liable to fines of up to $434,281, up from the existing limit of $173,998. The higher fines will also apply to fraudulent text messages and voice mails that tell people they have won a prize. Many thousands of dial−up Internet users have fallen victim to rogue dialers throughout 2005. Once installed on a dial−up user's PC, the applications can secretly dial a premium−rate number. This has led some people to run up call charges of hundreds of pounds. It's thought that many rogue dialers are spread using Trojan horses contained within spam e−mails. Last month, Ofcom warned that there was "growing evidence of consumer harm" arising from rogue dialers.
Source: http://news.com.com/British+rogue+dialers+face+heftier+fines/2100−1037_3−6005760.html?tag=cd.lede

33. *December 22, Tech Web* — **Symantec says vulnerability impacts 63 products.** Symantec on Wednesday, December 21, named more than 60 of its products as affected by the critical vulnerability disclosed earlier this week, and said it was pushing out a "heuristic" detection that would spot potential exploits. However, no patches have yet been released. The number of impacted products was among the largest ever for a single vulnerability, and demonstrated the risk of reusing code in a large group of programs. The bug, which was made public Tuesday, December 20, by researcher Alex Wheeler, is in how Symantec's AntiVirus Library, part of virtually all the Cupertino, CA,−based security giant's programs, handles RAR compressed files. RAR files are created by the WinRAR compression utility, developed and sold by RarLab. In an advisory released Wednesday, Symantec listed 48 enterprise titles and 15 consumer products that used the flawed Library. On the consumer side, the 2006 versions of Norton AntiVirus, Internet Security, SystemWorks, and Personal Firewall are open to attack. Corporate titles such as Norton AntiVirus for Microsoft Exchange, BrightMail Antispam, and AntiVirus for Handhelds are also on the list. The only protection for the moment is a special detection capability that Symantec is downloading to users' systems.
Source: http://www.securitypipeline.com/news/175007890;jsessionid=2AK0KWQB2SDV0QSNDBCSKH0CJUMEKJVN

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a third party report of multiple heap buffer overflows in the Symantec RAR decompression library (Dec2RAR.dll). Although there is limited information concerning this reported vulnerability, US−CERT encourages users and system administrators to consider filtering or disabling the scanning of RAR archives at email or proxy gateways. However, disabling RAR scanning may compromise the effectiveness of the security product. In addition, blocking RAR archives may prevent legitimate information from entering the network. By using a specially crafted RAR archive, a remote attacker may be able to perform any of the following malicious activities:

*Execute arbitrary code, possibly SYSTEM privileges
*Cause a denial of service condition, possibly disabling antivirus capabilities
*Take complete control of a vulnerable system

More information can be found in US−CERT Vulnerability Note VU#305272, Symantec RAR decompression library contains multiple heap overflows: http://www.kb.cert.org/vuls/id/305272

Current Port Attacks

Top 10 Target Ports	

	1026 (win−rpc), 4142 (oidocsvc), 445 (microsoft−ds), 27015 (halflife), 25 (smtp), 80 (www), 32789 (−−−), 53 (domain), 135 (epmap), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

34. *December 26, Agence France−Presse* — **Gas capsules with timers found in Russian stores.** Gas capsules with timers attached were found in stores in Saint Petersburg, the Russian city where dozens of people fell ill after inhaling an unknown gas that spread through a store, officials said. "The devices that were discovered consisted of capsules of gas with a strong garlicky smell. Clocks set to the current time were attached," a spokesperson for the Federal Security Service in Saint Petersburg told Agence France−Presse on Monday, December 26. Only in one of the three stores, all belonging to the Maksidom chain, did a capsule release gas, officials said. Dozens of people felt sick after inhaling the substance, with 16 hospitalized. Source: http://cnn.netscape.cnn.com/news/story.jsp?id=20051226093570 00000001&dt=20051226093500&w=AFP&coview=

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer